

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-202167

(P2001-202167A)

(43) 公開日 平成13年7月27日 (2001.7.27)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト*(参考)
G 0 6 F 1/32		G 0 6 F 12/00	5 3 1 M 5 B 0 1 1
12/00	5 3 1		5 3 7 H 5 B 0 1 7
	5 3 7	12/14	3 2 0 B 5 B 0 1 8
12/14	3 2 0	12/16	3 4 0 F 5 B 0 1 9
12/16	3 4 0		3 4 0 Q 5 B 0 8 2

審査請求 未請求 請求項の数 8 O L (全 6 頁) 最終頁に続く

(21) 出願番号 特願2000-11609(P2000-11609)

(22) 出願日 平成12年1月20日 (2000.1.20)

(71) 出願人 000003104

東洋通信機株式会社

神奈川県高座郡寒川町小谷2丁目1番1号

(72) 発明者 市瀬 浩

神奈川県高座郡寒川町小谷2丁目1番1号

東洋通信機株式会社内

(72) 発明者 黒沢 和雄

神奈川県高座郡寒川町小谷2丁目1番1号

東洋通信機株式会社内

(74) 代理人 100098039

弁理士 遠藤 恭

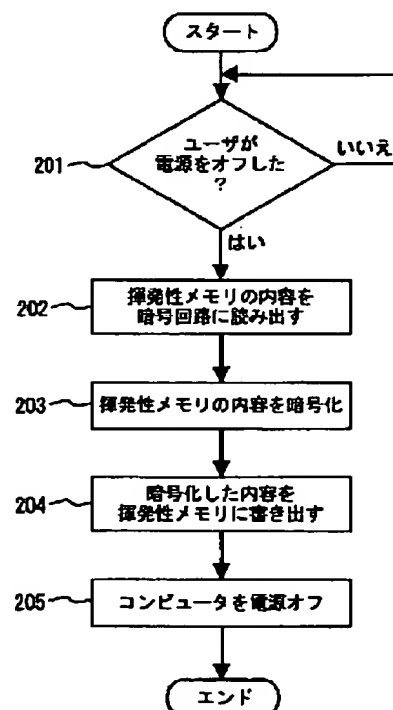
最終頁に続く

(54) 【発明の名称】 コンピュータ及びその制御方法

(57) 【要約】

【課題】 コンピュータ内のメモリを、他のコンピュータに取り付けられてもその内容を取得することができないような機能を備えたコンピュータ及びその制御方法を提供する。

【解決手段】 本発明は、コンピュータの電源をオフする指令があった場合、又はコンピュータを省電力モードに移行する指令があった場合に、コンピュータ内のメモリの内容を暗号化する工程と、該コンピュータが次に電源オン、又は省電力モードを解除する際にコンピュータ内の揮発性メモリの内容を復号化する工程と、前記2種の信号を受けてコンピュータ内の揮発性メモリの内容を暗号化、又は復号化する暗号回路16と、暗号化、又は復号化が完了したことを通知する暗号復号開始指示完了信号を備える。



【特許請求の範囲】

【請求項1】 入力データを暗号化する暗号化手段と、
入力データを復号化する復号化手段と、
コンピュータの電源をオフする指令があった場合、又は
コンピュータを省電力モードに移行する指令があった場合
に、前記暗号化手段によりコンピュータのメモリ上の
データを暗号化する暗号化制御手段と、
前記暗号化された、又は復号化されたデータをメモリ上
に格納する書き込み制御手段と、
前記データの格納が完了した後に、コンピュータ内機器 10
への電力供給を制限する電力制御手段と、
コンピュータの電源をオンする指令、又は省電力モード
を解除する指令があった場合に、前記暗号化されたデー
タを復号化する復号化制御手段と、を備えたコンピュ
ータ。

【請求項2】 前記暗号化手段により暗号化されるデー
タが、揮発性メモリ上のデータである請求項1に記載の
コンピュータ。

【請求項3】 バックアップ電源を更に備え、前記揮発
性メモリは前記電源オフの間、該バックアップ電源により 20
電力供給される請求項2に記載のコンピュータ。

【請求項4】 前記暗号化手段により暗号化されたデー
タを、補助記憶装置上に格納する請求項1又は2に記載
のコンピュータ。

【請求項5】 前記暗号化手段により暗号化されるデー
タが、補助記憶装置上のデータである請求項4に記載の
コンピュータ。

【請求項6】 前記暗号化手段により暗号化されるデー
タが、補助記憶装置上の読み出しのためのヘッダデータ 30
である請求項5に記載のコンピュータ。

【請求項7】 コンピュータの電源をオフする指令、又
はコンピュータを省電力モードに移行する指令があった
場合に、コンピュータのメモリ上のデータを暗号化する
工程と、

前記暗号化されたデータをメモリ上に格納する工程と、
前記データの格納が完了した後に、コンピュータ内機器
への電力供給を制限する工程と、を備えたコンピュータ
の制御方法。

【請求項8】 コンピュータの電源をオンする指令、又
は前記省電力モードを解除する指令があった場合に、前 40
記暗号化されたデータを復号化する工程と、
前記復号化されたデータをメモリ上に格納して、コンピ
ュータを使用可能な状態にする工程と、を更に備えた請
求項7に記載のコンピュータの制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、機密保持の機能を
備えたコンピュータ及びその制御方法に関し、特にコン
ピュータの電源オフ中に、メモリ上のデータを不特定他
者から保護する機能を備えたコンピュータ及びその制御 50

方法に関する。

【0002】

【従来の技術】近年、ノート型パソコンよりも更に小さ
くて軽い、情報端末と呼ばれる携帯性に優れたコンピュ
ータが普及しつつある。この種のコンピュータは、パソ
コンでは一般的な補助記憶装置であるハードディスクを
装備せず、内蔵の揮発性メモリにプログラムとデータを
格納して移動するため、コンピュータの更なる小型化、
軽量化、消費電力の低下を実現し、携帯性の向上を図っ
ている。しかし、揮発性メモリは絶えず電力供給しなけ
れば内容を失う記憶媒体であるため、この種のコンピュ
ータでは通常のパソコンのように完全な電源のオフがで
きず、電源スイッチをオフにした状態でも、内蔵の揮発
性メモリには電力を供給し続ける方式となっている。

【0003】この種のコンピュータにおける電源のオン
オフ制御について、図4を用いて説明する。ユーザが電
源スイッチ10に電源をオフする操作を与えると、一時
停止信号が割込信号発生回路11へ送られ、これに基づ
き、割込信号発生回路11は割込信号をCPU12へ送
る。CPU12は、揮発性メモリ13の特定番地に一時
停止状態を示す符号を書き込んだ後、電源オフ指示信号
を主電源14へ送る。主電源14は、これに従って電力
供給を停止し、割込信号発生回路11、CPU12、揮
発性メモリ13への電源供給は無くなる。一方で、揮発
性メモリ13だけはバックアップ電源15からの電源線
により電力が供給される。以上の手順を経て該コンピュ
ータは、電源をオフする。

【0004】ユーザが電源スイッチ10に電源をオンす
る操作を与えると、一時停止解除信号が主電源14へ送
られる。主電源14は、これに従って電力供給を開始
し、割込信号発生回路11、CPU12、揮発性メモリ
13への電源供給が始まる。CPU12は、揮発性メモ
リ13の特定番地を参照し、それが一時停止状態を示す
符号の場合はこれを削除した後、コンピュータを使用可
能な状態にする。

【0005】

【発明が解決しようとする課題】ところで、このような
小型のコンピュータは、携帯性が優れているが故に利用
者によって持ち歩かれる機会が多いので、置き忘れや紛
失、盗難により不特定他者の手に渡る可能性が高くな
る。そこで、コンピュータ内の揮発性メモリの内容が不
特定他者に知られないように電源オンの際にパスワード
の入力を求め、正しいパスワードが入力されない限り、
コンピュータが起動しないことによって機密性を確保す
る方法が一般的に知られている。しかしながら、揮発性
メモリへの電力供給を確保した状態でコンピュータ内か
ら揮発性メモリを取り出し、他のコンピュータでその内
容を取得することは可能であり、パスワードの入力のみ
ではその機密性を完全に保証することは困難である。

【0006】本発明の目的は、コンピュータ内の揮発性

メモリを、他のコンピュータに取り付けられてもその内容を取得することができないような機能を備えたコンピュータ、及びその制御方法を提供することにある。

【0007】

【課題を解決するための手段】前記目的を達成するために、本発明のコンピュータは、入力データを暗号化する暗号化手段と、入力データを復号化する復号化手段と、コンピュータの電源をオフする指令があった場合、又はコンピュータを省電力モードに移行する指令があった場合に、前記暗号化手段によりコンピュータのメモリ上のデータを暗号化する暗号化制御手段と、前記暗号化された、又は復号化されたデータをメモリ上に格納する書き込み制御手段と、前記データの格納が完了した後に、コンピュータ内機器への電力供給を切断する電力制御手段と、コンピュータの電源をオンする指令、又は省電力モードを解除する指令があった場合に、前記暗号化されたデータを復号化する復号化制御手段とを備えて構成される。

【0008】この場合に、前記暗号化手段により暗号化されるデータが、揮発性メモリ上のデータであることが好ましい。

【0009】更に、本発明は、バックアップ電源を更に備え、前記揮発性メモリが前記電源オフの間、該バックアップ電源により電力供給されるものが好ましい。

【0010】また、本発明は、前記暗号化手段により暗号化されたデータを、補助記憶装置上に格納する構成をすることができる。

【0011】この場合に、前記暗号化手段により暗号化されるデータが、補助記憶装置上のデータであることができる。

【0012】更に、前記暗号化手段により暗号化されるデータが、補助記憶装置上の読み出しのためのヘッダデータであることができる。

【0013】また、本発明のコンピュータの制御方法は、コンピュータの電源をオフする指令、又はコンピュータを省電力モードに移行する指令があった場合に、コンピュータのメモリ上のデータを暗号化する工程と、前記暗号化されたデータをメモリ上に格納する工程と、前記データの格納が完了した後に、コンピュータ内機器への電力供給を切断する工程と、を備えて構成される。

【0014】更に、本発明の制御方法は、コンピュータの電源をオンする指令、又は前記省電力モードを解除する指令があった場合に、前記暗号化されたデータを復号化する工程と、前記復号化されたデータをメモリ上に格納して、コンピュータを使用可能な状態にする工程と、を更に備えて構成することができる。

【0015】

【発明の実施の形態】以下、図示した一実施形態に基づいて本発明を詳細に説明する。図1は、本発明の一実施形態に係るコンピュータのブロック図である。図1に示

すように本実施形態に係るコンピュータは、電源スイッチ10、CPUへの割込信号を発生する割込信号発生回路11、CPU12、プログラムとデータを格納する揮発性メモリ13、コンピュータ内の全ての機器に電力を供給する主電源14、揮発性メモリにのみ電力を供給するバックアップ電源15、データの暗号化と復号化を行う暗号回路16を備えて構成される。

【0016】ここで暗号回路16は、CPU12を介して揮発性メモリ13の特定番地を除く領域の内容を読み込み、暗号化した内容に書き換える機能と、前記暗号化された揮発性メモリ13の特定番地を除く領域の内容を読み込み、復号化した内容に書き換える機能とを有する。暗号回路16で用いられる暗号化アルゴリズムとして、周知の種々のアルゴリズムを使用でき、従って前記アルゴリズムが公開鍵を用いた公開鍵方式に従うものであっても、秘密鍵を用いた秘密鍵方式に従うものであっても良く、更に、前記暗号回路16で用いられる暗号形式が、ストリーム暗号形式に従うものであっても、ブロック暗号形式に従うものであっても良い。また、暗号回路16は、ハードウェアの回路装置であっても、ソフトウェアでその機能を実現しても良い。

【0017】次に、本実施形態に係るコンピュータの電源のオンオフ制御について説明する。最初に図1及び図2に従って、コンピュータが電源オンの状態からユーザが電源をオフした場合の制御について説明する。ユーザが電源スイッチ10に電源をオフする操作を与えると

(201)、一時停止信号20が割込信号発生回路11へ送られ、これに基づき、割込信号発生回路11は割込信号21をCPU12へ送る。CPU12は、暗号復号開始指示信号24による暗号指示を暗号回路16へ送る。暗号回路16は、この暗号指示に従ってCPU12とバス30を介して揮発性メモリ13の特定番地を除く領域の内容を暗号化する。暗号回路16における暗号化は、メモリの内容を読み出して(202)、ビット単位でこれを暗号化し(203)、元のメモリの番地に暗号化したビット列を書き出す(204)ことにより行われる。暗号回路16は、この暗号化を完了後、暗号復号開始指示完了信号25をCPU12へ送る。CPU12は、揮発性メモリ13の特定番地に一時停止状態を示す符号を書き込んだ後、電源オフ指示信号22を主電源14へ送る。主電源14は、これに従って電源線40、41、42、44の電力供給を停止し、割込信号発生回路11、CPU12、揮発性メモリ13、暗号回路16への電源供給はなくなる(205)。一方で、揮発性メモリ13だけはバックアップ電源15からの電源線43で電力が供給される。以上の手順を経て該コンピュータは、電源をオフする。

【0018】以上の動作により、電源オフ時には、実際に電源がオフされる前にメモリ内のデータが暗号化される。このため、その暗号化ルールを知り得ない第三者

が、コンピュータから該メモリを取り出してその内容を読み出そうと試みた場合でも、これを解読できず、そのコンピュータのデータに対する高度なセキュリティが確保される。

【0019】次に、図1及び図3に従って、コンピュータが電源オフの状態からユーザが電源をオンした場合の制御について説明する。前記手順により電源がオフされたコンピュータに対し、ユーザが電源スイッチ10に電源をオンする操作を与えると(301)、一時停止解除信号23が主電源14へ送られる。主電源14は、これに従って電源線40、41、42、44の電力供給を開始し、割込信号発生回路11、CPU12、揮発性メモリ13、暗号回路16への電源供給が始まる。CPU12は、揮発性メモリ13の特定番地を参照し、これが一時停止状態を示す符号の場合は、ユーザにパスワードを要求する(302)。ユーザのパスワード入力が確認された場合(303)、CPU12はパスワードの適合性を判断し(304)、パスワードが適合した場合、CPU12は暗号復号開始指示信号24による復号指示を暗号回路16へ送る。暗号回路16は、これに従ってCPU12とバス30を介して揮発性メモリ13の特定番地を除く領域の内容を復号化する。暗号回路16における復号化は、メモリの内容を読み出して(305)、ビット単位でこれを復号化し(306)、元のメモリの番地に復号化したビット列を書き出す(307)ことにより行われる。暗号回路16は、この復号化を完了後、暗号復号開始指示完了信号25をCPU12へ送る。CPU12は、これに従って揮発性メモリ13の特定番地の一時停止状態を示す符号を削除後、コンピュータを使用可能な状態にする(308)。

【0020】以上、本発明の一実施形態を図面に沿って説明した。しかしながら本発明は上記実施形態に示した事項に限定されず、特許請求の範囲の記載に基いてその変更、改良等が可能であることは明らかである。上記実施形態においては、情報端末を対象として本発明を説明した。しかしながら本発明が対象とするコンピュータは、このような情報端末に限らず、ノート型パソコン及び据え置き型パソコンなどであっても良い。また、上記実施形態においては、電源オフ時を対象として本発明を説明した。しかしながら本発明が対象とする実行契機は、このような電源オフ時に限らず、省電力モード時などであっても良い。コンピュータが省電力モードに移行する際は、通常対象データを暗号化したのち、該モードの設定に従って、所定のコンピュータ内機器(例えばハ

ードディスクやティスプレイ)への電力供給を切断する。また、上記実施形態においては、揮発性メモリ上の内容を対象として本発明を説明した。しかしながら本発明が対象とする暗号化の内容は、このような揮発性メモリ上の内容に限らず、ハードディスク、MO(Magneto-Optical disc)、MD(Mini Disc)等の補助記憶装置上の内容であっても良い。尚、大容量の記憶領域を有する補助記憶装置の場合は、データを全て暗号化していると電源オフ時及び起動時に長時間かかるので、補助記憶装置上の読み出しのためのヘッダデータのみを暗号化を施すようにしても良い。また、上記実施形態においては、暗号化した内容を書き出す記憶媒体に揮発性メモリを対象として本発明を説明した。しかしながら本発明が対象とする記憶媒体は、このような揮発性メモリに限らず、補助記憶装置などであっても良い。更に、上記実施形態においては、暗号化された内容を復号化する工程でユーザにパスワードを要求する機能があることを対象として本発明を説明した。本発明が対象とするパスワードの入力方法は、キー入力をはじめ、各種認識手段であっても良い。

【0021】

【発明の効果】以上の如く本発明によれば、コンピュータの電源がオフの間、又は省電力モードの間は、揮発性メモリ上のデータは暗号化された状態で保存されるので、コンピュータ内の揮発性メモリを取り外して他のコンピュータに取り付けたとしても、その内容を取得することができないようになる。

【図面の簡単な説明】

【図1】 本発明の一実施形態に係るコンピュータの電源オンオフ制御に係るブロック図である。

【図2】 暗号化処理の制御を示すフローチャートである。

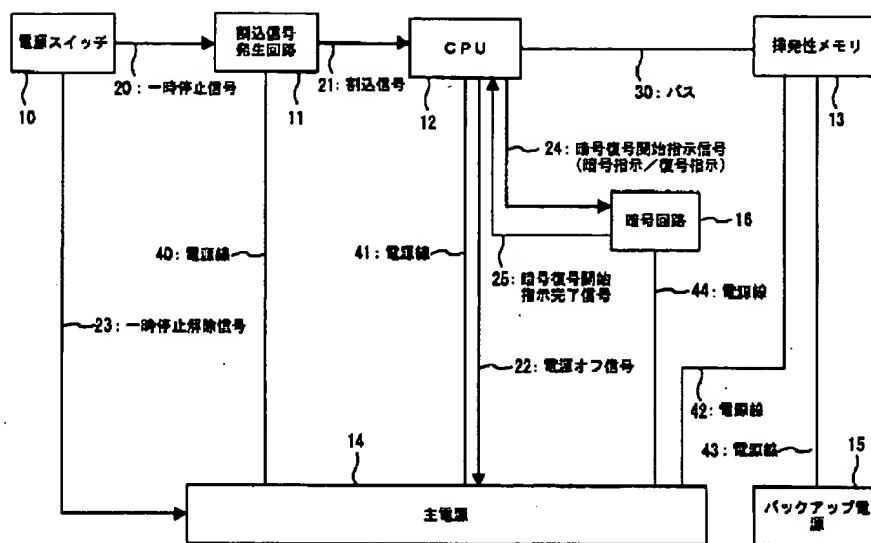
【図3】 復号化処理の制御を示すフローチャートである。

【図4】 従来のコンピュータの電源オンオフ制御に係るブロック図である。

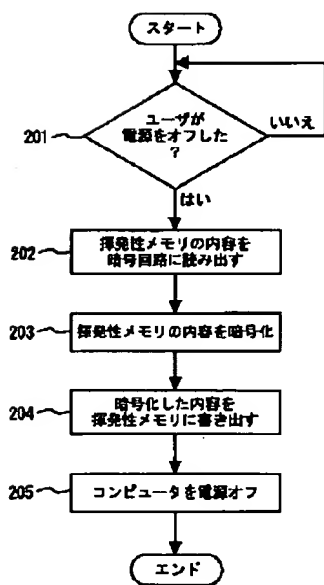
【符号の説明】

- 10 電源スイッチ
- 11 割込信号発生回路
- 12 CPU
- 13 揮発性メモリ
- 14 主電源
- 15 バックアップ電池
- 16 暗号回路

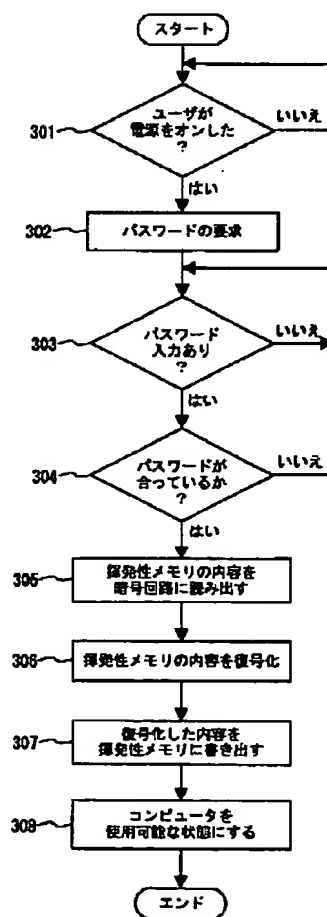
【図1】



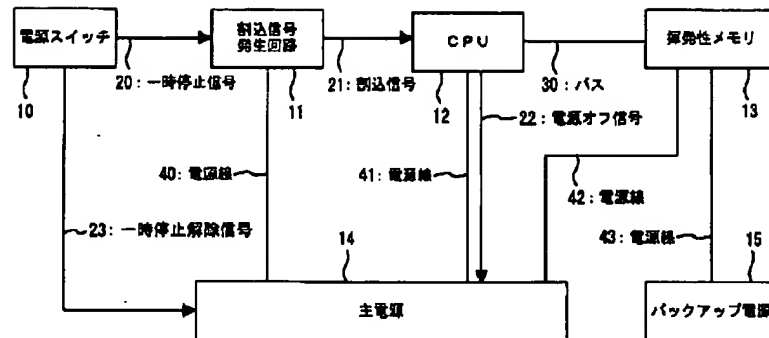
【図2】



【図3】



【図4】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 12/16	3 4 0	G 0 6 F 15/02	3 0 5 M
15/02	3 0 5	1/00	3 3 2 Z

(72)発明者 石井 清二
 神奈川県高座郡寒川町小谷2丁目1番1号
 東洋通信機株式会社内

Fターム(参考) 5B011 EA04 EB01 LL06 MB13
 5B017 AA07 BA05 BA07 BB03 BB10
 CA07 CA09 CA11 CA16
 5B018 GA10 JA26 KA02 KA03 LA01
 LA07 MA12 MA15 QA05 RA11
 5B019 CA08 CA10 HB10 HF01 HF10
 5B082 DA02 EA12 GA02

DERWENT-ACC-NO: 2001-526582

DERWENT-WEEK: 200158

COPYRIGHT 2005 DERWENT INFORMATION LTD

TITLE: Control method for computer e.g. notebook
personal computer, involves encrypting and decoding data
on memory
based on power supply ON/OFF and saving mode
command

PRIORITY-DATA: 2000JP-0011609 (January 20, 2000)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE
PAGES MAIN-IPC		
JP 2001202167 A	July 27, 2001	N/A
006 G06F 001/32		

INT-CL (IPC): G06F001/32, G06F012/00 , G06F012/14 , G06F012/16 ,
G06F015/02

ABSTRACTED-PUB-NO: JP2001202167A

BASIC-ABSTRACT:

NOVELTY - The data on the memory are encrypted when there is a
command for
turning the power supply OFF or operating computer in power saving
mode. The
power supply is limited after storing encrypted data. When a command
for power
supply ON and for releasing power saving mode is produced, the
encrypted data
are decoded.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for
computer.

USE - For computer e.g. notebook personal computer (PC).

ADVANTAGE - Since the data are encrypted or decoded based on command
of supply
ON/OFF or power saving mode, the data on the volatile memory are
preserved

efficiently.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart explaining the computer control. (Drawing includes non-English language text).

----- KWIC -----

Basic Abstract Text - ABTX (1):

NOVELTY - The data on the memory are encrypted when there is a command for turning the power supply OFF or operating computer in power saving mode. The power supply is limited after storing encrypted data. When a command for power supply ON and for releasing power saving mode is produced, the encrypted data are decoded.

Derwent Accession Number - NRAN (1):

2001-526582

Title - TIX (1):

Control method for computer e.g. notebook personal computer, involves encrypting and decoding data on memory based on power supply ON/OFF and saving mode command